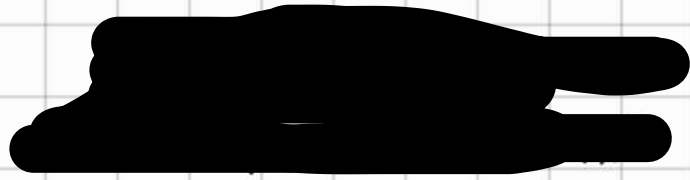


6 250

20



1.1A

ה IP של Host A, Host B ושל  
10.9.0.5, 10.9.0.6 ואיך  
הוא יתקדם.

אכן בכל השלש המכונות  
מבוצע אותו דבר.

במסגרת אישור התעבורה  
2 הודעות פנימיות וקבוצה 2 הודעות  
בזמן (עלוקה) וכן באמצעות  
לפחות 4 הודעות.

ואולי בקוד השלישי סתם.

אפשר לראות שהוא יגיע את  
SRC - דסט של הפקט.  
אז זה באמצעות הודעות  
שבו.

בפעם השנייה נסיונו איננו  
הרשאות כי אין לנו הרשאות  
כאנחנו משתמשים בה  
השראות וכמו שאנו יודעים  
מהטעות קודמת כי קטור  
לחצית הפעלה ואכן חייב  
הרשאות מנהל.

```
seed@VM: ~/Labsetup
[01/04/22]seed@VM:~/Labsetup$ dcup
Starting hostA-10.9.0.5 ... done
Starting seed-attacker ... done
Starting hostB-10.9.0.6 ... done
Attaching to seed-attacker, hostA-10.9.0.5, hostB-10.9.0.6
hostA-10.9.0.5 | * Starting internet superserver inetd
hostB-10.9.0.6 | * Starting internet superserver inetd
^CGracefully stopping... (press Ctrl+C again to force)
Stopping hostA-10.9.0.5 ... done
Stopping hostB-10.9.0.6 ... done
Stopping seed-attacker ... done
[01/04/22]seed@VM:~/Labsetup$ dcup
Starting hostB-10.9.0.6 ... done
Starting hostA-10.9.0.5 ... done
Starting seed-attacker ... done
Attaching to seed-attacker, hostA-10.9.0.5, hostB-10.9.0.6
hostA-10.9.0.5 | * Starting internet superserver inetd
hostB-10.9.0.6 | * Starting internet superserver inetd
```

No.	Time	Source	Destination	Protocol	Length	Info
1	2022-01-04 15:13:10.100	10.9.0.5	10.9.0.6	ICMP	64	80 bytes from 10.9.0.5: icmp_seq=1 ttl=64 time=0.066 ms
2	2022-01-04 15:13:10.100	10.9.0.6	10.9.0.5	ICMP	64	80 bytes from 10.9.0.5: icmp_seq=2 ttl=64 time=0.117 ms
3	2022-01-04 15:13:10.100	10.9.0.5	10.9.0.6	ICMP	64	80 bytes from 10.9.0.5: icmp_seq=3 ttl=64 time=0.066 ms

```
seed@VM: ~/volumes
[01/04/22]seed@VM:~/volumes$ ping 10.9.0.5
PING 10.9.0.5 (10.9.0.5): 56(84) bytes of data:
64 bytes from 10.9.0.5: icmp_seq=1 ttl=64 time=0.066 ms
64 bytes from 10.9.0.5: icmp_seq=2 ttl=64 time=0.117 ms
^C
--- 10.9.0.5 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 0.066/0.091/0.117/0.025 ms
[01/04/22]seed@VM:~/volumes$
```

```
seed@VM: ~/volumes
[01/04/22]seed@VM:~/volumes$ sudo python3 shiffer1.1A.py
sniffing packets
###[ Ethernet ]###
dst      = 02:42:0a:09:00:05
src      = 02:42:97:b3:2e:71
type     = IPv4
###[ IP ]###
version  = 4
ihl      = 5
tos      = 0x0
len      = 84
id       = 39544
flags    = DF
frag     = 0
ttl      = 64
proto    = icmp
chksum   = 0x8c19
src      = 10.9.0.1
dst      = 10.9.0.5
\options
###[ ICMP ]###
type     = echo-request
code     = 0
chksum   = 0x2979
id       = 0x3
seq      = 0x1
###[ Raw ]###
```

```
seed@VM: ~/volumes
[01/04/22]seed@VM:~/volumes$ python3 sniffer1.1A.py
sniffing packets
Traceback (most recent call last):
  File "sniffer1.1A.py", line 8, in <module>
    packet = sniff(iface = "br-ae32e9ad3ed5", filter = "icmp", prn= print_pkt)
  File "/usr/local/lib/python3.8/dist-packages/scapy/sendrecv.py", line 1036, in sniff
    sniffer._run(*args, **kwargs)
  File "/usr/local/lib/python3.8/dist-packages/scapy/sendrecv.py", line 906, in run
    sniff_sockets[L2socket(type=ETH_P_ALL, iface=iface,
  File "/usr/local/lib/python3.8/dist-packages/scapy/arch/linux.py", line 398, in __init__
    self.ins = socket.socket(socket.AF_PACKET, socket.SOCK_RAW, socket.htons(type)) # noqa: E501
  File "/usr/lib/python3.8/socket.py", line 231, in __init__
    _socket.socket._init(self, family, type, proto, fileno)
PermissionError: [Errno 1] Operation not permitted
[01/04/22]seed@VM:~/volumes$
```

1.1B:

```
seed@VM: ~/./volumes
[01/04/22] seed@VM:~/./volumes$ sudo python3 shiffer1.1A.py
sniffing packets
###[ Ethernet ]###
  dst      = 02:42:0a:09:00:05
  src      = 02:42:97:b3:2e:71
  type     = IPv4
###[ IP ]###
  version  = 4
  ihl      = 5
  tos      = 0x0
  len      = 84
  id       = 39544
  flags    = DF
  frag     = 0
  ttl      = 64
  proto    = icmp
  chksum   = 0x8c19
  src      = 10.9.0.1
  dst      = 10.9.0.5
  options  \
###[ ICMP ]###
  type     = echo-request
  code     = 0
  chksum   = 0x2979
  id       = 0x3
  seq      = 0x1
###[ Raw ]###
```

אניגה א ק פקטור קמא לכונו כה  
 ב - 111 הנו צינע ק לפטור לפטור סוף  
 ב.

```
[01/06/22] seed@VM:~/./volumes$ sudo python3 sniffer1.1B.py
sniffing packets
###[ Ethernet ]###
  dst      = 52:54:00:12:35:02
  src      = 08:00:27:04:01:83
  type     = IPv4
###[ IP ]###
  version  = 4
  ihl      = 5
  tos      = 0x0
  len      = 84
  id       = 28243
  flags    = DF
  frag     = 0
  ttl      = 64
  proto    = icmp
  chksum   = 0xb037
  src      = 10.9.0.1
  dst      = 8.8.8.8
  options  \
###[ ICMP ]###
  type     = echo-request
  code     = 0
  chksum   = 0x9bc3
  id       = 0x5
  seq      = 0x1
###[ Raw ]###
  load     = 'G\x98\xd6a\x00\x00\x00\x00s1\x0c\x00\x00\x00\x00\x00\x00\x10\x11\x12\x13\x14\x15\
  !"#%&'()*+,-./01234567'
###[ Ethernet ]###
```

אז העקר א אופס א קו  
 נסיון נס אלא ק בקי  
 אק כאן אלא אלא אופס  
 אלא אלא אופס א ק 8.8.8.8

```
1 from scapy.all import *
2 print("sniffing packets")
3
4 def print_pkt(pkt):
5     pkt.show()
6
7 # (filter = "icmp", prn= print_pkt)# part 1
8 packet = sniff(iface = "br-ae32e9ad3ed5", filter = "tcp", prn=
9     print_pkt) #part 2
9 # packet = sniff(filter = "icmp and host 8.8.8.8", prn= print_pkt)
10 # part 3
```

```
seed@VM: ~/./volumes
seed@VM:~/./volumes
  flags    = DF
  frag     = 0
  ttl      = 64
  proto    = tcp
  chksum   = 0x3d85
  src      = 10.9.0.5
  dst      = 10.9.0.1
  options  \
###[ TCP ]###
  sport     = telnet
  dport     = 41514
  seq       = 1784407128
  ack       = 1309346890
  dataofs   = 8
  reserved  = 0
  flags     = PA
  window    = 509
  chksum    = 0x1453
  urgptr    = 0
  options   = [('NOP', None), ('NOP', None)]
53302453]]
###[ Raw ]###
  load     = 'seed@153b7cbbd2e:-$ '
```

כין אלא אלא  
 אופס א  
 הפקטור סוף  
 קצת. אלא בנויה  
 Telnet  
 אלא יוקס א לפה אלק  
 סר קצת.

## Task 1.2

כדי שאפשר להאזין בתוכנית  
אלו הפורטים את אדס.  
מכיוון שאנו ב-10.9.0.1  
ולכן ל-10.9.0.0.  
אפשר להאזין בולטאין  
שמו התקבל תשובה בחזרה  
למחשב שלי. אז קיים.  
אין לו את האיש.  
לחלוקה האחרונה אפשר להאזין  
באתר שיתפסו ה-אדס  
שאי השתנה. מכיוון שמחשבי  
ל- hostA. אס. הינו פריטים  
למאסין loopback.

```
seed@VM: ~/volumes
[01/06/22]seed@VM:~/volumes$ sudo python3
Python 3.8.5 (default, Jul 28 2020, 12:59:40)
[GCC 9.3.0] on linux
Type "help", "copyright", "credits" or "license()" for more information.
>>> a=IP()
Traceback (most recent call last):
  File "<stdin>", line 1, in <module>
NameError: name 'IP' is not defined
>>> s.src = '10.9.0.0'
Traceback (most recent call last):
  File "<stdin>", line 1, in <module>
NameError: name 's' is not defined
>>> a.src = '10.9.0.0'
Traceback (most recent call last):
  File "<stdin>", line 1, in <module>
NameError: name 'a' is not defined
>>> a.dest = '10.9.0.6'
Traceback (most recent call last):
  File "<stdin>", line 1, in <module>
NameError: name 'a' is not defined
>>> from scapy.all import *
>>> a = IP('10.9.0.0')
>>> a.src = '10.9.0.0'
>>> b = ICMP()
>>> p = a/b
>>> send(p)
Sent 1 packets.
>>> send(p)
```

No.	Time	Source	Destination	Protocol	Length	Info
1	2022-01-06 04:12	10.9.0.0	127.0.0.1	ICMP	42	Echo (ping) request 10:0x0000, seq=0/0, ttl=64 (no response ...)





```
seed@VM: ~/volumes
proto      : ByteEnumField      = 0      (0)
chksum     : XShortField        = None   (None)
src        : SourceIPField      = '10.0.2.15' (None)
dst        : DestIPField        = '172.217.171.206' (None)
options    : PacketListField    = []     ([])
.
Sent 1 packets.
[01/06/22]seed@VM:~/../volumes$ sudo python3 Task1.3.py
version    : BitField (4 bits)  = 4      (4)
ihl        : BitField (4 bits)  = None   (None)
tos        : XByteField         = 0      (0)
len        : ShortField         = None   (None)
id         : ShortField         = 1      (1)
flags      : FlagsField (3 bits) = <Flag 0 (> (<Flag 0 (>))
frag       : BitField (13 bits) = 0      (0)
ttl        : ByteField          = 9      (64)
proto      : ByteEnumField      = 0      (0)
chksum     : XShortField        = None   (None)
src        : SourceIPField      = '10.0.2.15' (None)
dst        : DestIPField        = '172.217.171.206' (None)
options    : PacketListField    = []     ([])
.
Sent 1 packets.
[01/06/22]seed@VM:~/../volumes$
```

## Task 1.4

```
Task1.4.py
1 from scapy.all import *
2
3 def spoof(pkt):
4     if ICMP in pkt and pkt[ICMP].type == 8:
5         print('start sniff')
6         print('original source:', pkt[IP].src)
7         print('original dest:', pkt[IP].dst)
8
9         ip = IP(src=pkt[IP].dst, dst=pkt[IP].src, ihl=pkt[IP].ihl)
10        icmp = ICMP(type=8, id=pkt[ICMP].id, seq=pkt[ICMP].seq)
11        data = pkt[Raw].load
12        newpkt = ip/icmp/data
13
14        print('spoof')
15        print('spoof source:', newpkt[IP].src)
16        print('spoof dest:', newpkt[IP].dst)
17        send(newpkt, verbose=0)
18
19 packet = sniff(filter='br-a3226a3d3e05', filter='icmp', promiscuous=True)
20
21 [1]+  Stopped                  ping 10.9.0.5
[01/06/22]seed@VM:~/../volumes$
```

```
64 bytes from 10.9.0.5: icmp_seq=13 ttl=64 time=0.117 ms
64 bytes from 10.9.0.5: icmp_seq=14 ttl=64 time=0.126 ms
64 bytes from 10.9.0.5: icmp_seq=15 ttl=64 time=0.120 ms
64 bytes from 10.9.0.5: icmp_seq=16 ttl=64 time=0.098 ms
64 bytes from 10.9.0.5: icmp_seq=17 ttl=64 time=0.098 ms
^C
--- 10.9.0.5 ping statistics ---
17 packets transmitted, 17 received, 0% packet loss, time 1634
rtt min/avg/max/mdev = 0.090/0.126/0.260/0.037 ms
[01/06/22]seed@VM:~/../volumes$ ping 10.9.0.5
PING 10.9.0.5 (10.9.0.5) 56(84) bytes of data.
64 bytes from 10.9.0.5: icmp_seq=1 ttl=64 time=0.100 ms
64 bytes from 10.9.0.5: icmp_seq=1 ttl=64 time=24.2 ms (DUP!)
64 bytes from 10.9.0.5: icmp_seq=2 ttl=64 time=0.139 ms
64 bytes from 10.9.0.5: icmp_seq=2 ttl=64 time=13.2 ms (DUP!)
64 bytes from 10.9.0.5: icmp_seq=3 ttl=64 time=0.121 ms
64 bytes from 10.9.0.5: icmp_seq=3 ttl=64 time=12.6 ms (DUP!)
64 bytes from 10.9.0.5: icmp_seq=4 ttl=64 time=0.131 ms
64 bytes from 10.9.0.5: icmp_seq=4 ttl=64 time=6.23 ms (DUP!)
64 bytes from 10.9.0.5: icmp_seq=5 ttl=64 time=0.127 ms
64 bytes from 10.9.0.5: icmp_seq=5 ttl=64 time=12.8 ms (DUP!)
^Z
[1]+  Stopped                  ping 10.9.0.5
[01/06/22]seed@VM:~/../volumes$
```

No.	Time	Source	Destination	Protocol	Length	Info
1	2022-01-06 08:41:10.9.0.1	10.9.0.1	10.9.0.5	ICMP	80	Echo (ping) request 10.9.0.0.0.0. seq=8/2848, ttl=64 (reply in ...)
2	2022-01-06 08:41:10.9.0.5	10.9.0.5	10.9.0.1	ICMP	80	Echo (ping) reply 10.9.0.0.0.0. seq=8/2848, ttl=64 (reply in ...)
3	2022-01-06 08:41:10.9.0.1	10.9.0.1	10.9.0.5	ICMP	80	Echo (ping) request 10.9.0.0.0.0. seq=9/2904, ttl=64 (request i...
4	2022-01-06 08:41:10.9.0.5	10.9.0.5	10.9.0.1	ICMP	80	Echo (ping) reply 10.9.0.0.0.0. seq=9/2904, ttl=64 (reply in ...)
5	2022-01-06 08:41:10.9.0.1	10.9.0.1	10.9.0.5	ICMP	80	Echo (ping) request 10.9.0.0.0.0. seq=10/2960, ttl=64 (request i...
6	2022-01-06 08:41:10.9.0.5	10.9.0.5	10.9.0.1	ICMP	80	Echo (ping) reply 10.9.0.0.0.0. seq=10/2960, ttl=64 (reply in ...)
7	2022-01-06 08:41:10.9.0.1	10.9.0.1	10.9.0.5	ICMP	80	Echo (ping) request 10.9.0.0.0.0. seq=11/3016, ttl=64 (request i...
8	2022-01-06 08:41:10.9.0.5	10.9.0.5	10.9.0.1	ICMP	80	Echo (ping) reply 10.9.0.0.0.0. seq=11/3016, ttl=64 (reply in ...)
9	2022-01-06 08:41:10.9.0.1	10.9.0.1	10.9.0.5	ICMP	80	Echo (ping) request 10.9.0.0.0.0. seq=12/3072, ttl=64 (request i...
10	2022-01-06 08:41:10.9.0.5	10.9.0.5	10.9.0.1	ICMP	80	Echo (ping) reply 10.9.0.0.0.0. seq=12/3072, ttl=64 (reply in ...)
11	2022-01-06 08:41:10.9.0.1	10.9.0.1	10.9.0.5	ICMP	80	Echo (ping) request 10.9.0.0.0.0. seq=13/3128, ttl=64 (request i...
12	2022-01-06 08:41:10.9.0.5	10.9.0.5	10.9.0.1	ICMP	80	Echo (ping) reply 10.9.0.0.0.0. seq=13/3128, ttl=64 (reply in ...)
13	2022-01-06 08:41:10.9.0.1	10.9.0.1	10.9.0.5	ICMP	80	Echo (ping) request 10.9.0.0.0.0. seq=14/3184, ttl=64 (request i...
14	2022-01-06 08:41:10.9.0.5	10.9.0.5	10.9.0.1	ICMP	80	Echo (ping) reply 10.9.0.0.0.0. seq=14/3184, ttl=64 (reply in ...)
15	2022-01-06 08:41:10.9.0.1	10.9.0.1	10.9.0.5	ICMP	80	Echo (ping) request 10.9.0.0.0.0. seq=15/3240, ttl=64 (request i...
16	2022-01-06 08:41:10.9.0.5	10.9.0.5	10.9.0.1	ICMP	80	Echo (ping) reply 10.9.0.0.0.0. seq=15/3240, ttl=64 (reply in ...)
17	2022-01-06 08:41:10.9.0.1	10.9.0.1	10.9.0.5	ICMP	80	Echo (ping) request 10.9.0.0.0.0. seq=16/3296, ttl=64 (request i...
18	2022-01-06 08:41:10.9.0.5	10.9.0.5	10.9.0.1	ICMP	80	Echo (ping) reply 10.9.0.0.0.0. seq=16/3296, ttl=64 (reply in ...)

```
Frame 1: 90 bytes on wire (784 bits), 90 bytes captured (784 bits) on interface br-a3226a3d3e05, id 0
Ethernet II, Src: 02:42:ad:bd:f2:0f (02:42:ad:bd:f2:0f), Dst: 02:42:8a:99:00:05 (02:42:8a:99:00:05)
Internet Protocol Version 4, Src: 10.9.0.1, Dst: 10.9.0.5
.
[01/06/22]seed@VM:~/../volumes
[01/06/22]seed@VM:~/../volumes$ ^C
[01/06/22]seed@VM:~/../volumes$ sudo python3 Task1.4.py
start sniff
original source: 10.9.0.1
original dest: 10.9.0.5
spoof
spoof source: 10.9.0.5
spoof dest: 10.9.0.1
start sniff
original source: 10.9.0.1
original dest: 10.9.0.5
spoof
spoof source: 10.9.0.5
spoof dest: 10.9.0.1
start sniff
original source: 10.9.0.1
original dest: 10.9.0.5
spoof
spoof source: 10.9.0.5
spoof dest: 10.9.0.1
start sniff
original source: 10.9.0.1
original dest: 10.9.0.5
spoof
```

על מנת להגן על האתר  
Host B - ping  
ואם נשאלים בדבר אולי  
שמולד בין השרת והקליין  
אשר האתר אולי  
בהצפנה וזה בקוד,  
האני חשבה לפקטור  
ובקלות אולי חשבה  
חשבה וזהלש בין  
src - dest



## Task 2.1A

```
seed@VM: ~/volumes
[01/06/22]seed@VM:~/../volumes$ ping 10.9.0.5
PING 10.9.0.5 (10.9.0.5) 56(84) bytes of data.
54 bytes from 10.9.0.5: icmp_seq=1 ttl=64 time=0.052 ms
54 bytes from 10.9.0.5: icmp_seq=2 ttl=64 time=0.060 ms
54 bytes from 10.9.0.5: icmp_seq=3 ttl=64 time=0.058 ms
^C
[1]+  Stopped                  ping 10.9.0.5
[01/06/22]seed@VM:~/../volumes$
```

```
seed@VM: ~/volumes
[01/06/22]seed@VM:~/../volumes$ sudo ./sniffer
Got a packet
Source IP is: 10.9.0.1
Destination IP is: 10.9.0.5
Got a packet
Source IP is: 10.9.0.5
Destination IP is: 10.9.0.1
Got a packet
Source IP is: 10.9.0.1
Destination IP is: 10.9.0.5
Got a packet
Source IP is: 10.9.0.5
Destination IP is: 10.9.0.1
Got a packet
Source IP is: 10.9.0.1
Destination IP is: 10.9.0.5
Got a packet
Source IP is: 10.9.0.5
Destination IP is: 10.9.0.1
```

Q1) כפי שראינו קודם את  
src ip ו-dest ip אנחנו צריכים לשלוח  
פקטת ping אל שרתנו ונראה שיש לנו  
את ה-dest ip ו-  
את ה-src ip.

Q2) אנחנו חייבים להראות שה-2 שונים  
לפי כפי שהיו ב-ethernet (ה-2 שונים והיו  
לפי).

Q3) אנחנו חייבים להראות שה-2 שונים  
לפי Ethernet, icmp, ו-  
ה-2 שונים.

Q4) אנחנו חייבים להראות שה-2 שונים  
לפי Ethernet, icmp, ו-  
ה-2 שונים.

```
h
e
/
=
Got a packet

***** ICMP Packet *****
Source IP is: 10.9.0.1
Destination IP is: 10.9.0.6
ICMP Echo type is: Type 8 Echo Request
ICMP Echo code is: 0
Got a packet

***** ICMP Packet *****
Source IP is: 10.9.0.6
Destination IP is: 10.9.0.1
ICMP Echo type is: Type 0 Echo Reply
ICMP Echo code is: 0
Got a packet

d
h
e
0
e
Got a packet

***** ICMP Packet *****
Source IP is: 10.9.0.1
Destination IP is: 10.9.0.6
ICMP Echo type is: Type 8 Echo Request
ICMP Echo code is: 0
Got a packet

***** ICMP Packet *****
Source IP is: 10.9.0.6
Destination IP is: 10.9.0.1
ICMP Echo type is: Type 0 Echo Reply
ICMP Echo code is: 0

[2]+ Stopped                  ping 10.9.0.6
[01/06/22]seed@VM:~/../volumes$
```

## Task 2.1B

אנחנו חייבים להראות כי  
ה-2 שונים בין  
10.9.0.1  
בין 10.9.0.6, ונראה שיש לנו  
ה-2 שונים.

```

seed@VM: ~/volumes
***** TCP Packet *****
Source IP is: 10.9.0.1
Destination IP is: 10.9.0.6
Source Port is: 59580
Destination Port is: 23
Got a packet

***** TCP Packet *****
Source IP is: 10.9.0.1
Destination IP is: 10.9.0.6
Source Port is: 59580
Destination Port is: 23
Got a packet

***** TCP Packet *****
Source IP is: 10.9.0.1
Destination IP is: 10.9.0.6
Source Port is: 59580
Destination Port is: 23
Got a packet

***** TCP Packet *****
Source IP is: 10.9.0.1
Destination IP is: 10.9.0.6
Source Port is: 59580
Destination Port is: 23
Got a packet

```

```

seed@VM: ~/volumes
This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Thu Jan 6 18:46:44 UTC 2022 from 10.9.0.1 on pts/2
seed@61faa7elf08a:~$ exit
logout
Connection closed by foreign host.
[01/06/22]seed@VM:~/volumes$ telnet 10.9.0.6
Trying 10.9.0.6...
Connected to 10.9.0.6.
Escape character is '^'.
Ubuntu 20.04.1 LTS
61faa7elf08a login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Thu Jan 6 18:51:19 UTC 2022 from 10.9.0.1 on pts/2
seed@61faa7elf08a:~$ exit
logout
Connection closed by foreign host.
[01/06/22]seed@VM:~/volumes$

```

```

***** TCP Packet *****
Source IP is: 10.9.0.1
Destination IP is: 10.9.0.6
Source Port is: 59596
Destination Port is: 23
Data:
D?000d
Got a packet

***** TCP Packet *****
Source IP is: 10.9.0.1
Destination IP is: 10.9.0.6
Source Port is: 59596
Destination Port is: 23
Data:
C?000e
Got a packet

***** TCP Packet *****
Source IP is: 10.9.0.1
Destination IP is: 10.9.0.6
Source Port is: 59596
Destination Port is: 23
Data:
?000s
Got a packet

```

אשלי אדואר טן כי אין התעלה  
 מ. החלק השני כולו האזניות  
 1-100-100 port כפחיתות  
 TCP. אשלי זלזלתי כי אשלי  
 שכן הסנפיר אשלי חברים אשלי

Tas/2.1C  
 TCP data אשלי אשלי  
 אשלי אשלי אשלי אשלי  
 אשלי אשלי



Task 2.2A

Task 2.2B

עליו חסר של המשימה  
 זייכנו קיפ אפסר אפסר  
 בתחילה מאתנו רשום  
 אפסר ping אק ה אפסר  
 לא תואם אפסר אפסר  
 זולל לא משהב אק  
 הוא קיבל אק היקטלה.

The image shows a Wireshark packet capture on the left and a terminal window on the right. The terminal shows a series of commands and their outputs in a VM environment.

```

[01/06/22] seed@VM: ~/.../volumes$ sudo ./Task2.2A
bash: sudo./Task2.2A: No such file or directory
[01/06/22] seed@VM: ~/.../volumes$ ls
a.out main.py Task2.1A.c Task2.1BB task2.1.
BB.pcap task2.1B.pcap Task2.2A.c
Core sniffer Task2.1B Task2.1BB.c Task2.1B
.c Task2.2A Task2.2A.pcap
[01/06/22] seed@VM: ~/.../volumes$ sudo ./Task2.2A
sent ICMP request to 8.8.8.8
[01/06/22] seed@VM: ~/.../volumes$
    
```

The Wireshark capture shows an ICMP Echo (ping) request from 10.0.2.15 to 8.8.8.8. The packet details show the ICMP type as 8 (Echo) and the length as 60 bytes.

א) אם מכין שמה אם תשלח בקטנה יותר קטנה הוא ירד אותה באפס'ים  
 על מנת שיהיה תודה באפס' הודו'.

ב) אנו חייבים לחשב את ממש check כמחר אנו מתחילים  
 ב- sockets שלח. כפי בואר להחזיר לקום הודו' של קי  
 ואי נאסות (המשלח) בזכרים במחש' (5).

ג) אנו חייבים להשתמש בהרשאה שלח data, cmp, ip, Ethernet  
 המורכב הפסלה.  
 מכיון שאנו נאשים לאיזר בו המורכב הפסלה שלח מתחילים עליו  
 אנו חייבים הרשאה שלח sockets שלח אלא שלח רוקים בעצמנו  
 להקדיש את הרשאה.

ping 10.9.0.5

```
sent ICMP reply to 10.9.0.6
sent ICMP reply to 10.9.0.6
```

אבסר לראות כי אלה  
 שלמים נ HostA  
 - HostB את icmp  
 ה את Attacker שולח  
 / את הגישה לפני  
 / את והקבלה בין  
 src - dst ואלו  
 אבסר להיות עם האשמה  
 ע"ן תצורה לבקשת icmp.  
 מנה את התקלות  
 - 09.05 - 10.06